Exhibit N

EXHIBIT B-1
Invalidity of U.S. Patent No. 8,924,543 in view of Jain

European Patent Application No. EP1143665A2 ("Jain") was filed on December 6, 2000 and published on October 10, 2001, and therefore constitutes prior art under at least 35 U.S.C. §§ 102(a) and (b) as to the Asserted Claims of U.S. Patent No. 8,924,543 ("the '543 Patent"). Jain anticipates and/or renders obvious the Asserted Claims, either alone or in combination with one or more references identified in Defendants' Cover Pleading.

To the extent Plaintiff argues that Jain does not disclose any element below, a person of ordinary skill in the art would have found it obvious in view of Jain alone, with the knowledge of a person of ordinary skill in the art, and/or in view of the prior art systems and references disclosed in § II of Defendants' Invalidity Contentions and the exemplary citations and commentary provided for this claim in Exhibits B-1 to B-8 and Appendix B-B thereto. A person of ordinary skill in the art would have been motivated to combine and would have a reasonable expectation of success in combining these references because the cited references relate to the same technical field as Jain (i.e., network management).

The chart below provides representative examples of where each element is found within Jain. Citations are meant to be exemplary, not exhaustive, and Defendants reserve the right to identify and discuss additional portions of the reference in support of its contentions and/or to rebut arguments made by Plaintiff. Citations to figures, drawings, tables, and the like include reference to any accompanying or related text. All internal cross references are meant to incorporate the cross-referenced material as if fully set forth therein.

It is Defendants' position that Plaintiff's Disclosure of Asserted Claims and Infringement Contentions have not established that any accused product or service infringes any valid claim. Thus, Defendants' statements below should not be treated as an admission, implication, or suggestion that Defendants agree with Plaintiff regarding either the scope, construction, or interpretation of any of the Asserted Claims of the infringement theories advanced by Plaintiff in its Preliminary Infringement Contentions, including whether any Asserted Claims satisfies 35 U.S.C. §§ 101 or 112. In certain cases, Defendants specify non-limiting examples of where its application of the prior art is based on Plaintiff's apparent application of the claim element. These statements are not intended to suggest that Defendants agree with Plaintiff's application of any claim term, suggest a proposed construction at this stage of the case, or suggest that construction is needed, as the parties are not required to exchange terms for construction or proposed constructions until a later date.

Plaintiff has yet to identify of the Asserted Claims that it contends is not anticipated and/or rendered obvious by Jain. Defendants therefore expressly reserve the right to respond to any such contention, including by identifying additional obviousness combinations, if Plaintiff makes any such contention.

Where Defendants state that Jain "discloses" a limitation, that disclosure may be express, implicit, and/or inherent.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

U.S. Patent No. US 8,924,543 (the "'543 Patent")	
Claim Language	**Exemplary Disclosure**
[1p] A network service plan provisioning system communicatively coupled to a wireless end-user device over a wireless access network, the network service plan provisioning system comprising one or more network elements configured to:	Jain discloses a network service plan provisioning system communicatively coupled to a wireless end-user device over a wireless access network, the network service plan provisioning system comprising one or more network elements configured to. *See, e.g.*: [0007] The present invention is directed to a unified policy management system where various policies, namely, the set of rules and instructions that determine the network=s operation, may be established and enforced from a single site. According to one embodiment of the invention, the system includes a first edge device associated with a first network having a first set of resources that is configured to manage the policies for the first network according to the policy settings stored in a first database. The system also includes a second edge device associated with a second network having a second set of resources that is configured to manage the policies for the second network according to the policy settings stored in a second database. The first and second edge devices act as policy enforcers for their respective networks. The policies being enforced may include firewall policies, VPN policies, and the like. [0008] The system further includes a central policy server in communication with the first and second edge devices. The policy server is configured to define the first and second policy settings and manage the first and second edge devices from a single location. Thus, a network administrator need not multiply his or her efforts and associated expenditures in configuring and managing the policy enforcers individually. [0017] The functionalities of the policy enforcers in enforcing the policies for their respective networks may also be partitioned for effective hardware implementation. According to one embodiment of the invention, each edge device preferably includes a plurality of modules including a classification engine, a policy engine, and a packet forwarding engine. The classification engine determines a protocol associated with an incoming packet. The policy engine makes a forwarding decision for the packet based on policy settings associated with the packet. The packet forwarding module then forwards the packet based on the policy settings. [Cl. 1] In a system including a first edge device managing policies for a first network according to first policy settings and a second edge device managing policies for a second network according to second policy settings, the system further including a central policy server in communication with the

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	first and second edge devices configured to define the first and second policy settings and manage the first and second edge devices from a single location, each edge device comprising: a classification engine for determining a protocol associated with an incoming packet; a policy engine for making a forwarding decision for the packet based on policy settings associated with the packet; and a packet forwarding module for forwarding the packet based on the policy settings.
	[0030] Local network 102 includes a policy server 122 for defining and managing network services and policies for the organization. The network policies are a set of rules and instructions that determine the network=s operation, such as firewall, VPN, bandwidth, and administration policies. The firewall policies decide the network traffic that is to be allowed to flow from the public Internet 108 into the local networks 102, 104, and the traffic that is to be blocked. The bandwidth policies determine the kind of bandwidth that is to be allocated to the traffic flowing through the local networks. The VPN policies determine the rules for implementing multiple site connectivity across the local networks. The administration policies decide the users that have access to administrative functions, the type of administrative functions allocated to these users, and the policy enforcers 124, 126 on which these users may exercise such administrative functions. The firewall, VPN, bandwidth, and administration policies for the entire organization are preferably stored in a policy server database 130 maintained by the policy server 122. **[0031]** Each local network 102, 104 also includes an edge device, referred to as a policy enforcer 124, 126, for controlling access to the network. Each policy enforcer 124, 126 manages the network policies and services for the users and resources of their respective local networks 102, 104, as permitted by the policy server 122. Respective portions of the policy server database 130 are copied to the policy enforcer databases 132, 134 for allowing the policy enforcers to manage the network policies and services for the local networks 102, 104. *See* **Jain Figs. 1, 3, 11, 18, 19** To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[1a] obtain and store a first service plan component and a second service plan component,	Jain discloses obtaining and storing a first service plan component and a second service plan component.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	See, e.g.: [0007] The present invention is directed to a unified policy management system where various policies, namely, the set of rules and instructions that determine the network=s operation, may be established and enforced from a single site. According to one embodiment of the invention, the system includes a first edge device associated with a first network having a first set of resources that is configured to manage the policies for the first network according to the policy settings stored in a first database. The system also includes a second edge device associated with a second network having a second set of resources that is configured to manage the policies for the second network according to the policy settings stored in a second database. The first and second edge devices act as policy enforcers for their respective networks. The policies being enforced may include firewall policies, VPN policies, and the like. [0008] The system further includes a central policy server in communication with the first and second edge devices. The policy server is configured to define the first and second policy settings and manage the first and second edge devices from a single location. Thus, a network administrator need not multiply his or her efforts and associated expenditures in configuring and managing the policy enforcers individually. [0017] The functionalities of the policy enforcers in enforcing the policies for their respective networks may also be partitioned for effective hardware implementation. According to one embodiment of the invention, each edge device preferably includes a plurality of modules including a classification engine, a policy engine, and a packet forwarding engine. The classification engine determines a protocol associated with an incoming packet. The policy engine makes a forwarding decision for the packet based on policy settings associated with the packet. The packet forwarding module then forwards the packet based on the policy settings. [0030] Local network 102 includes a policy server 122 for defining and managing network services and policies for the organization. The network policies are a set of rules and instructions that determine the network=s operation, such as firewall, VPN, bandwidth, and administration policies. The firewall policies decide the network traffic that is to be allowed to flow from the public Internet 108 into the local networks 102, 104, and the traffic that is to be blocked. The bandwidth policies determine the kind of bandwidth that is to be allocated to the traffic flowing through the local networks. The VPN policies determine the rules for implementing multiple site connectivity across the local networks. The administration policies decide the users that have access to administrative functions, the type of administrative functions allocated to these users, and the policy enforcers 124,

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

126 on which these users may exercise such administrative functions. The firewall, VPN, bandwidth, and administration policies for the entire organization are preferably stored in a policy server database 130 maintained by the policy server 122.

[0031] Each local network 102, 104 also includes an edge device, referred to as a policy enforcer 124, 126, for controlling access to the network. Each policy enforcer 124, 126 manages the network policies and services for the users and resources of their respective local networks 102, 104, as permitted by the policy server 122. Respective portions of the policy server database 130 are copied to the policy enforcer databases 132, 134 for allowing the policy enforcers to manage the network policies and services for the local networks 102, 104.

[0033] According to one embodiment of the invention, a policy object 222 includes a bandwidth policy 224, firewall policy 226, administration policy 228, and VPN policy 230. The VPN policy 230 defines a security policy for the member networks and includes one or more VPN clouds 232. Each VPN cloud 232 is an individual VPN or a group of VPNs defining a security policy group which includes a list of sites 234 and users 236 who can communicate with each other. A site is preferably a set of hosts/networks physically located behind one of the policy enforcers 124, 126. In other words, a site is a definition of a network which includes the policy enforcer that is associated with it. The policy enforcers for the sites act as VPN tunnel endpoints once the hosts under the sites start communicating. These communications are governed by a set of rules 238 configured for each VPN cloud. The rules 238 may govern, among other things, VPN access permissions and security features such as the level of encryption and authentication used for the connectivity at the network layer.

[0045] FIG. 3 is a more detailed schematic block diagram of the policy server 122 according to one embodiment of the invention. The policy server 122 preferably includes a management module 302 that allows centralized control over the policy enforcers 124, 126 from a single console. The policy server 122 further includes a log collecting and archiving module 304 and a policy server reports module 316. The log collecting and archiving module 304 collects information about the status and usage of resources from the policy enforcers 124, 126 as well as from the management module 302, and stores them in an archive database 318. The policy server reports module 316 uses the collected logs and archives to generate reports in an organized report format.

[0047] The centralized management sub-module 306 enables a network administrator to install and manage individual policy enforcers from a central location. The network administrator preferably uses a web-based graphical user interface to define the policy enforcer's network configuration and

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	monitor various aspects of the device, such as device health, device alarms, VPN connection status, and the like.
	[0048] The policy management sub-module 308 provides the network administrator with the ability to create policies that span multiple functional aspects of the policy enforcer (e.g. firewall, bandwidth management, and virtual private networks), multiple resources (e.g. users, hosts, services and time), and multiple policy enforcers.
	[0057] Referring again to FIG. 4, the centralized management sub-module 306 also includes a global monitor user interface 402 and a data collector program 412, respectively displaying and collecting the health and status of all the policy enforcers managed by the policy server 122. The data collector program 412 receives health and status information from each of the up-and-running policy enforcers it manages, and passes the relevant information to the global monitor user interface. A health agent running as a daemon in each of the policy enforcers being monitored periodically collects data from the device and analyzes its health status. The collected data is then transferred to the policy server 122 when requested by the data collector program 412.
	[0059] Referring again to FIG. 3, the policy management sub-module 308 allows for policy management of the policy enforcers 124, 126. As discussed above, all policy management functions are implemented in terms of resource objects stored in the policy databases 130, 132, 134 including users, devices, hosts, services, and time. Preferably, all resources are associated with default policy settings selected by the administrator during the installation process. The network administrator views, adds, and modifies the policies centrally via a graphical user interface provided by the policy management sub-module 308. This allows for a policy-centric management model where the administrator is given the impression that a single logical server provides the firewall, bandwidth management, and VPN services across the enterprise. The fact that the policy is enforced on individual policy enforcers in different locations is transparent to the administrator.
	[0070] According to one embodiment of the invention, each firewall policy includes a policy identifier (ID) attribute 724 for identifying a particular policy rule in the list of policies. An order number attribute 726 for the policy rule indicates the sequence in which the policy is to be applied. In this regard, the policy enforcer 124, 126 for the local network takes one rule at a time, in sequence, compares it against the network traffic, and preferably applies the first rule that matches the network traffic.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

| | [0071] Each firewall policy also includes a description attribute 728 for describing the firewall policy to be applied. For instance, the description may indicate that the policy allows spam blocking, URL blocking, VPN key management, and the like. An action flag attribute 730 indicates whether traffic is to be allowed or denied for the indicated policy. An active flag attribute 732 indicates whether the policy has been activated or de-activated. Thus, the network administrator may create a policy and activate it at a later time. A policy that has been de-activated preferably has no effect on the network traffic.

[0072] Each firewall policy further includes a user attribute 734, source attribute 736, service attribute 738, destination attribute (not shown), and time attribute (not shown). Each of these attributes is preferably represented by a group name or a resource name. The name acts as a pointer to an entry in the group root object 202 or resource root object of the LDAP database 130, 132, or 134.

[0078] Referring again to FIG. 8, selection of the bandwidth tab 720c allows the display, addition, and modification of various bandwidth policies determining the kind of bandwidth to be allocated to a traffic flowing through a particular policy enforcer. Different bandwidths may be specified for different users, hosts, and services.

[0107] FIG. 18 is a schematic block diagram of the policy enforcer 124, 126 illustrating the partitioning of the various functionalities according to one embodiment of the invention. The policy enforcer includes an Internet protocol security (IPSec) engine 502 for performing security and authentication functions in implementing, for instance, virtual private networks. A stream table 506 assembles the packets passing through the policy enforcer into streams. A protocol classification engine 508 decodes the protocols used in forwarding the packets. A policy engine 510 enforces policies for the packets based on the policy settings stored in the policy database 132, 134. A packet forwarding module 504 receives packets from the public Internet via the router 110 and buffers, forwards, or drops the packets based on the policies being enforced. A bandwidth management module 514 provides bandwidth shaping services to the packets being forwarded based on the bandwidth settings stored in the policy database 132, 134.

[0108] In practice, an incoming packet is matched against the stream table 506 for determining if a matching entry already exists in the table. If not, a new entry is added. The stream table preferably includes enough portions of the packet to uniquely identify a stream. For example, in enforcing policies on IP layer three through layer four traffic, the stream table may store a source IP, destination IP, source port, destination port, and protocol number of the incoming packet. |

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

<table>
<tr>
<td></td>
<td>

[0109] The protocol classification engine 508 takes the new stream and obtains a detailed protocol decode for the stream. The policy engine 510 is then queried for the policy rules to be applied to the stream. Based on the policy rules returned by the policy engine 510, the packet forwarding module 504, IPSec engine 502, and/or the bandwidth management module 514 process the streams accordingly. The processing may be recursive until the packets in the stream have had all the actions specified by the policy rule set applied to them.

[0111] FIG. 19 is a more detailed schematic block diagram of the policy engine 510 according to one embodiment of the invention. The policy engine 510 includes a policy request table 602 that acts as a queue for all the policy decision requests. In this regard, the portion of the packet matching the information stored in the stream table 506 is presented to the policy engine 510 in the form of a policy request. The policy request is then queued in the policy request table 602.

[0112] A resource engine 604 maintains an up-to-date mapping of resource group names to member mappings. A policy rules database buffer 608 stores a current policy rule set to be applied by the policy engine 510. The policy rules stored in the buffer 608 are preferably in the original group-based rule specification format. Thus, the buffer 608 stores a rule created for a group in its group-based form instead of instantiating a rule for each member of the group.

[0113] A decision engine 606 includes logic to serve the incoming policy decision requests in the policy request table 602 by matching it against the policy rule set in the policy rules database buffer 608 based on the actual membership information obtained from the resource engine 604. The relevant group-based rule matching the traffic is then identified and decision bits in the stream table set for enforcing the corresponding actions. The decision bits thus constitute the set of actions to be performed on the packets of the stream. All packets matching the streams are then processed based on these decision bits. The decision engine may also specify an access control list (ACL) including a set of rules that allow/deny traffic, a DiffServ standard for providing a quality of service level to the traffic, and/or VPN implementation information.

[0133] The policy server 122 preferably stores the policy management information for all the policy enforcers in the policy server database 130. This information is organized in the databases 130 as one or more DNs with corresponding attributes. Appropriate portions of the policy server database are then copied to the policy enforcer databases 132, 134.

</td>
</tr>
</table>

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	[Cl. 1] In a system including a first edge device managing policies for a first network according to first policy settings and a second edge device managing policies for a second network according to second policy settings, the system further including a central policy server in communication with the first and second edge devices configured to define the first and second policy settings and manage the first and second edge devices from a single location, each edge device comprising: a classification engine for determining a protocol associated with an incoming packet; a policy engine for making a forwarding decision for the packet based on policy settings associated with the packet; and a packet forwarding module for forwarding the packet based on the policy settings.
	See **Jain Figs. 1, 3, 11, 18, 19**
	To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[1b] the first service plan component comprising (1) information specifying a first traffic classification filter for filtering a traffic event in a network traffic inspection system, the traffic event being associated with the wireless end-user device and (2) a first network policy enforcement action that is triggered in a network policy enforcement system when the traffic event possesses a characteristic that matches the first traffic classification filter, and the second service plan component comprising (a) information specifying a second traffic classification filter for filtering the traffic event in the network traffic inspection system, and (b) a second network policy enforcement action that is triggered in	Jain discloses the first service plan component comprising (1) information specifying a first traffic classification filter for filtering a traffic event in a network traffic inspection system, the traffic event being associated with the wireless end-user device and (2) a first network policy enforcement action that is triggered in a network policy enforcement system when the traffic event possesses a characteristic that matches the first traffic classification filter, and the second service plan component comprising (a) information specifying a second traffic classification filter for filtering the traffic event in the network traffic inspection system, and (b) a second network policy enforcement action that is triggered in the network policy enforcement system when the traffic event possesses a characteristic that matches the second traffic classification filter. *See, e.g.*: **[0007]** The present invention is directed to a unified policy management system where various policies, namely, the set of rules and instructions that determine the network=s operation, may be established and enforced from a single site. According to one embodiment of the invention, the system includes a first edge device associated with a first network having a first set of resources that is configured to manage the policies for the first network according to the policy settings stored in a first database. The system also includes a second edge device associated with a second network having a second set of resources that is configured to manage the policies for the second network

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

the network policy enforcement system when the traffic event possesses a characteristic that matches the second traffic classification filter;	according to the policy settings stored in a second database. The first and second edge devices act as policy enforcers for their respective networks. The policies being enforced may include firewall policies, VPN policies, and the like. [0008] The system further includes a central policy server in communication with the first and second edge devices. The policy server is configured to define the first and second policy settings and manage the first and second edge devices from a single location. Thus, a network administrator need not multiply his or her efforts and associated expenditures in configuring and managing the policy enforcers individually. [0017] The functionalities of the policy enforcers in enforcing the policies for their respective networks may also be partitioned for effective hardware implementation. According to one embodiment of the invention, each edge device preferably includes a plurality of modules including a classification engine, a policy engine, and a packet forwarding engine. The classification engine determines a protocol associated with an incoming packet. The policy engine makes a forwarding decision for the packet based on policy settings associated with the packet. The packet forwarding module then forwards the packet based on the policy settings. [0030] Local network 102 includes a policy server 122 for defining and managing network services and policies for the organization. The network policies are a set of rules and instructions that determine the network=s operation, such as firewall, VPN, bandwidth, and administration policies. The firewall policies decide the network traffic that is to be allowed to flow from the public Internet 108 into the local networks 102, 104, and the traffic that is to be blocked. The bandwidth policies determine the kind of bandwidth that is to be allocated to the traffic flowing through the local networks. The VPN policies determine the rules for implementing multiple site connectivity across the local networks. The administration policies decide the users that have access to administrative functions, the type of administrative functions allocated to these users, and the policy enforcers 124, 126 on which these users may exercise such administrative functions. The firewall, VPN, bandwidth, and administration policies for the entire organization are preferably stored in a policy server database 130 maintained by the policy server 122. [0031] Each local network 102, 104 also includes an edge device, referred to as a policy enforcer 124, 126, for controlling access to the network. Each policy enforcer 124, 126 manages the network policies and services for the users and resources of their respective local networks 102, 104, as permitted by the policy server 122. Respective portions of the policy server database 130 are copied

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	to the policy enforcer databases 132, 134 for allowing the policy enforcers to manage the network policies and services for the local networks 102, 104. **[0033]** According to one embodiment of the invention, a policy object 222 includes a bandwidth policy 224, firewall policy 226, administration policy 228, and VPN policy 230. The VPN policy 230 defines a security policy for the member networks and includes one or more VPN clouds 232. Each VPN cloud 232 is an individual VPN or a group of VPNs defining a security policy group which includes a list of sites 234 and users 236 who can communicate with each other. A site is preferably a set of hosts/networks physically located behind one of the policy enforcers 124, 126. In other words, a site is a definition of a network which includes the policy enforcer that is associated with it. The policy enforcers for the sites act as VPN tunnel endpoints once the hosts under the sites start communicating. These communications are governed by a set of rules 238 configured for each VPN cloud. The rules 238 may govern, among other things, VPN access permissions and security features such as the level of encryption and authentication used for the connectivity at the network layer. **[0045]** FIG. 3 is a more detailed schematic block diagram of the policy server 122 according to one embodiment of the invention. The policy server 122 preferably includes a management module 302 that allows centralized control over the policy enforcers 124, 126 from a single console. The policy server 122 further includes a log collecting and archiving module 304 and a policy server reports module 316. The log collecting and archiving module 304 collects information about the status and usage of resources from the policy enforcers 124, 126 as well as from the management module 302, and stores them in an archive database 318. The policy server reports module 316 uses the collected logs and archives to generate reports in an organized report format. **[0047]** The centralized management sub-module 306 enables a network administrator to install and manage individual policy enforcers from a central location. The network administrator preferably uses a web-based graphical user interface to define the policy enforcer's network configuration and monitor various aspects of the device, such as device health, device alarms, VPN connection status, and the like. **[0048]** The policy management sub-module 308 provides the network administrator with the ability to create policies that span multiple functional aspects of the policy enforcer (e.g. firewall, bandwidth management, and virtual private networks), multiple resources (e.g. users, hosts, services and time), and multiple policy enforcers.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

[0057] Referring again to FIG. 4, the centralized management sub-module 306 also includes a global monitor user interface 402 and a data collector program 412, respectively displaying and collecting the health and status of all the policy enforcers managed by the policy server 122. The data collector program 412 receives health and status information from each of the up-and-running policy enforcers it manages, and passes the relevant information to the global monitor user interface. A health agent running as a daemon in each of the policy enforcers being monitored periodically collects data from the device and analyzes its health status. The collected data is then transferred to the policy server 122 when requested by the data collector program 412. **[0059]** Referring again to FIG. 3, the policy management sub-module 308 allows for policy management of the policy enforcers 124, 126. As discussed above, all policy management functions are implemented in terms of resource objects stored in the policy databases 130, 132, 134 including users, devices, hosts, services, and time. Preferably, all resources are associated with default policy settings selected by the administrator during the installation process. The network administrator views, adds, and modifies the policies centrally via a graphical user interface provided by the policy management sub-module 308. This allows for a policy-centric management model where the administrator is given the impression that a single logical server provides the firewall, bandwidth management, and VPN services across the enterprise. The fact that the policy is enforced on individual policy enforcers in different locations is transparent to the administrator. **[0070]** According to one embodiment of the invention, each firewall policy includes a policy identifier (ID) attribute 724 for identifying a particular policy rule in the list of policies. An order number attribute 726 for the policy rule indicates the sequence in which the policy is to be applied. In this regard, the policy enforcer 124, 126 for the local network takes one rule at a time, in sequence, compares it against the network traffic, and preferably applies the first rule that matches the network traffic. **[0071]** Each firewall policy also includes a description attribute 728 for describing the firewall policy to be applied. For instance, the description may indicate that the policy allows spam blocking, URL blocking, VPN key management, and the like. An action flag attribute 730 indicates whether traffic is to be allowed or denied for the indicated policy. An active flag attribute 732 indicates whether the policy has been activated or de-activated. Thus, the network administrator may create a policy and activate it at a later time. A policy that has been de-activated preferably has no effect on the network traffic.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	[0072] Each firewall policy further includes a user attribute 734, source attribute 736, service attribute 738, destination attribute (not shown), and time attribute (not shown). Each of these attributes is preferably represented by a group name or a resource name. The name acts as a pointer to an entry in the group root object 202 or resource root object of the LDAP database 130, 132, or 134. **[0078]** Referring again to FIG. 8, selection of the bandwidth tab 720c allows the display, addition, and modification of various bandwidth policies determining the kind of bandwidth to be allocated to a traffic flowing through a particular policy enforcer. Different bandwidths may be specified for different users, hosts, and services. **[0107]** FIG. 18 is a schematic block diagram of the policy enforcer 124, 126 illustrating the partitioning of the various functionalities according to one embodiment of the invention. The policy enforcer includes an Internet protocol security (IPSec) engine 502 for performing security and authentication functions in implementing, for instance, virtual private networks. A stream table 506 assembles the packets passing through the policy enforcer into streams. A protocol classification engine 508 decodes the protocols used in forwarding the packets. A policy engine 510 enforces policies for the packets based on the policy settings stored in the policy database 132, 134. A packet forwarding module 504 receives packets from the public Internet via the router 110 and buffers, forwards, or drops the packets based on the policies being enforced. A bandwidth management module 514 provides bandwidth shaping services to the packets being forwarded based on the bandwidth settings stored in the policy database 132, 134. **[0108]** In practice, an incoming packet is matched against the stream table 506 for determining if a matching entry already exists in the table. If not, a new entry is added. The stream table preferably includes enough portions of the packet to uniquely identify a stream. For example, in enforcing policies on IP layer three through layer four traffic, the stream table may store a source IP, destination IP, source port, destination port, and protocol number of the incoming packet. **[0109]** The protocol classification engine 508 takes the new stream and obtains a detailed protocol decode for the stream. The policy engine 510 is then queried for the policy rules to be applied to the stream. Based on the policy rules returned by the policy engine 510, the packet forwarding module 504, IPSec engine 502, and/or the bandwidth management module 514 process the streams accordingly. The processing may be recursive until the packets in the stream have had all the actions specified by the policy rule set applied to them.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

[0111] FIG. 19 is a more detailed schematic block diagram of the policy engine 510 according to one embodiment of the invention. The policy engine 510 includes a policy request table 602 that acts as a queue for all the policy decision requests. In this regard, the portion of the packet matching the information stored in the stream table 506 is presented to the policy engine 510 in the form of a policy request. The policy request is then queued in the policy request table 602. [0112] A resource engine 604 maintains an up-to-date mapping of resource group names to member mappings. A policy rules database buffer 608 stores a current policy rule set to be applied by the policy engine 510. The policy rules stored in the buffer 608 are preferably in the original group-based rule specification format. Thus, the buffer 608 stores a rule created for a group in its group-based form instead of instantiating a rule for each member of the group. [0113] A decision engine 606 includes logic to serve the incoming policy decision requests in the policy request table 602 by matching it against the policy rule set in the policy rules database buffer 608 based on the actual membership information obtained from the resource engine 604. The relevant group-based rule matching the traffic is then identified and decision bits in the stream table set for enforcing the corresponding actions. The decision bits thus constitute the set of actions to be performed on the packets of the stream. All packets matching the streams are then processed based on these decision bits. The decision engine may also specify an access control list (ACL) including a set of rules that allow/deny traffic, a DiffServ standard for providing a quality of service level to the traffic, and/or VPN implementation information. [0133] The policy server 122 preferably stores the policy management information for all the policy enforcers in the policy server database 130. This information is organized in the databases 130 as one or more DNs with corresponding attributes. Appropriate portions of the policy server database are then copied to the policy enforcer databases 132, 134. [Cl. 1] In a system including a first edge device managing policies for a first network according to first policy settings and a second edge device managing policies for a second network according to second policy settings, the system further including a central policy server in communication with the first and second edge devices configured to define the first and second policy settings and manage the first and second edge devices from a single location, each edge device comprising: a classification engine for determining a protocol associated with an incoming packet; a policy engine for making a forwarding decision for the packet based on policy settings associated with the packet; and a packet forwarding module for forwarding the packet based on the policy settings.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	See **Jain Figs. 1, 3, 11, 18, 19** To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[1c] process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter, the network provisioning instruction set comprising one or more traffic inspection provisioning instructions for the network traffic inspection system and one or more policy enforcement provisioning instructions for the network policy enforcement system, the network traffic inspection system and the network policy enforcement system implementing one or more policies applicable to the wireless end-user device;	Jain discloses processing the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter, the network provisioning instruction set comprising one or more traffic inspection provisioning instructions for the network traffic inspection system and one or more policy enforcement provisioning instructions for the network policy enforcement system, the network traffic inspection system and the network policy enforcement system implementing one or more policies applicable to the wireless end-user device. *See, e.g.*: **[0007]** The present invention is directed to a unified policy management system where various policies, namely, the set of rules and instructions that determine the network=s operation, may be established and enforced from a single site. According to one embodiment of the invention, the system includes a first edge device associated with a first network having a first set of resources that is configured to manage the policies for the first network according to the policy settings stored in a first database. The system also includes a second edge device associated with a second network having a second set of resources that is configured to manage the policies for the second network according to the policy settings stored in a second database. The first and second edge devices act as policy enforcers for their respective networks. The policies being enforced may include firewall policies, VPN policies, and the like. **[0008]** The system further includes a central policy server in communication with the first and second edge devices. The policy server is configured to define the first and second policy settings and manage the first and second edge devices from a single location. Thus, a network administrator need not multiply his or her efforts and associated expenditures in configuring and managing the policy enforcers individually.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

| | [0017] The functionalities of the policy enforcers in enforcing the policies for their respective networks may also be partitioned for effective hardware implementation. According to one embodiment of the invention, each edge device preferably includes a plurality of modules including a classification engine, a policy engine, and a packet forwarding engine. The classification engine determines a protocol associated with an incoming packet. The policy engine makes a forwarding decision for the packet based on policy settings associated with the packet. The packet forwarding module then forwards the packet based on the policy settings.

[0030] Local network 102 includes a policy server 122 for defining and managing network services and policies for the organization. The network policies are a set of rules and instructions that determine the network=s operation, such as firewall, VPN, bandwidth, and administration policies. The firewall policies decide the network traffic that is to be allowed to flow from the public Internet 108 into the local networks 102, 104, and the traffic that is to be blocked. The bandwidth policies determine the kind of bandwidth that is to be allocated to the traffic flowing through the local networks. The VPN policies determine the rules for implementing multiple site connectivity across the local networks. The administration policies decide the users that have access to administrative functions, the type of administrative functions allocated to these users, and the policy enforcers 124, 126 on which these users may exercise such administrative functions. The firewall, VPN, bandwidth, and administration policies for the entire organization are preferably stored in a policy server database 130 maintained by the policy server 122.

[0031] Each local network 102, 104 also includes an edge device, referred to as a policy enforcer 124, 126, for controlling access to the network. Each policy enforcer 124, 126 manages the network policies and services for the users and resources of their respective local networks 102, 104, as permitted by the policy server 122. Respective portions of the policy server database 130 are copied to the policy enforcer databases 132, 134 for allowing the policy enforcers to manage the network policies and services for the local networks 102, 104.

[0033] According to one embodiment of the invention, a policy object 222 includes a bandwidth policy 224, firewall policy 226, administration policy 228, and VPN policy 230. The VPN policy 230 defines a security policy for the member networks and includes one or more VPN clouds 232. Each VPN cloud 232 is an individual VPN or a group of VPNs defining a security policy group which includes a list of sites 234 and users 236 who can communicate with each other. A site is preferably a set of hosts/networks physically located behind one of the policy enforcers 124, 126. In other words, a site is a definition of a network which includes the policy enforcer that is associated with it. The policy enforcers for the sites act as VPN tunnel endpoints once the hosts under the sites start |

16

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

| | communicating. These communications are governed by a set of rules 238 configured for each VPN cloud. The rules 238 may govern, among other things, VPN access permissions and security features such as the level of encryption and authentication used for the connectivity at the network layer.

[0045] FIG. 3 is a more detailed schematic block diagram of the policy server 122 according to one embodiment of the invention. The policy server 122 preferably includes a management module 302 that allows centralized control over the policy enforcers 124, 126 from a single console. The policy server 122 further includes a log collecting and archiving module 304 and a policy server reports module 316. The log collecting and archiving module 304 collects information about the status and usage of resources from the policy enforcers 124, 126 as well as from the management module 302, and stores them in an archive database 318. The policy server reports module 316 uses the collected logs and archives to generate reports in an organized report format.

[0047] The centralized management sub-module 306 enables a network administrator to install and manage individual policy enforcers from a central location. The network administrator preferably uses a web-based graphical user interface to define the policy enforcer's network configuration and monitor various aspects of the device, such as device health, device alarms, VPN connection status, and the like.

[0048] The policy management sub-module 308 provides the network administrator with the ability to create policies that span multiple functional aspects of the policy enforcer (e.g. firewall, bandwidth management, and virtual private networks), multiple resources (e.g. users, hosts, services and time), and multiple policy enforcers.

[0057] Referring again to FIG. 4, the centralized management sub-module 306 also includes a global monitor user interface 402 and a data collector program 412, respectively displaying and collecting the health and status of all the policy enforcers managed by the policy server 122. The data collector program 412 receives health and status information from each of the up-and-running policy enforcers it manages, and passes the relevant information to the global monitor user interface. A health agent running as a daemon in each of the policy enforcers being monitored periodically collects data from the device and analyzes its health status. The collected data is then transferred to the policy server 122 when requested by the data collector program 412.

[0059] Referring again to FIG. 3, the policy management sub-module 308 allows for policy management of the policy enforcers 124, 126. As discussed above, all policy management functions are implemented in terms of resource objects stored in the policy databases 130, 132, 134 including |

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	users, devices, hosts, services, and time. Preferably, all resources are associated with default policy settings selected by the administrator during the installation process. The network administrator views, adds, and modifies the policies centrally via a graphical user interface provided by the policy management sub-module 308. This allows for a policy-centric management model where the administrator is given the impression that a single logical server provides the firewall, bandwidth management, and VPN services across the enterprise. The fact that the policy is enforced on individual policy enforcers in different locations is transparent to the administrator. [0070] According to one embodiment of the invention, each firewall policy includes a policy identifier (ID) attribute 724 for identifying a particular policy rule in the list of policies. An order number attribute 726 for the policy rule indicates the sequence in which the policy is to be applied. In this regard, the policy enforcer 124, 126 for the local network takes one rule at a time, in sequence, compares it against the network traffic, and preferably applies the first rule that matches the network traffic. [0071] Each firewall policy also includes a description attribute 728 for describing the firewall policy to be applied. For instance, the description may indicate that the policy allows spam blocking, URL blocking, VPN key management, and the like. An action flag attribute 730 indicates whether traffic is to be allowed or denied for the indicated policy. An active flag attribute 732 indicates whether the policy has been activated or de-activated. Thus, the network administrator may create a policy and activate it at a later time. A policy that has been de-activated preferably has no effect on the network traffic. [0072] Each firewall policy further includes a user attribute 734, source attribute 736, service attribute 738, destination attribute (not shown), and time attribute (not shown). Each of these attributes is preferably represented by a group name or a resource name. The name acts as a pointer to an entry in the group root object 202 or resource root object of the LDAP database 130, 132, or 134. [0078] Referring again to FIG. 8, selection of the bandwidth tab 720c allows the display, addition, and modification of various bandwidth policies determining the kind of bandwidth to be allocated to a traffic flowing through a particular policy enforcer. Different bandwidths may be specified for different users, hosts, and services. [0107] FIG. 18 is a schematic block diagram of the policy enforcer 124, 126 illustrating the partitioning of the various functionalities according to one embodiment of the invention. The policy

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	enforcer includes an Internet protocol security (IPSec) engine 502 for performing security and authentication functions in implementing, for instance, virtual private networks. A stream table 506 assembles the packets passing through the policy enforcer into streams. A protocol classification engine 508 decodes the protocols used in forwarding the packets. A policy engine 510 enforces policies for the packets based on the policy settings stored in the policy database 132, 134. A packet forwarding module 504 receives packets from the public Internet via the router 110 and buffers, forwards, or drops the packets based on the policies being enforced. A bandwidth management module 514 provides bandwidth shaping services to the packets being forwarded based on the bandwidth settings stored in the policy database 132, 134. [0108] In practice, an incoming packet is matched against the stream table 506 for determining if a matching entry already exists in the table. If not, a new entry is added. The stream table preferably includes enough portions of the packet to uniquely identify a stream. For example, in enforcing policies on IP layer three through layer four traffic, the stream table may store a source IP, destination IP, source port, destination port, and protocol number of the incoming packet. [0109] The protocol classification engine 508 takes the new stream and obtains a detailed protocol decode for the stream. The policy engine 510 is then queried for the policy rules to be applied to the stream. Based on the policy rules returned by the policy engine 510, the packet forwarding module 504, IPSec engine 502, and/or the bandwidth management module 514 process the streams accordingly. The processing may be recursive until the packets in the stream have had all the actions specified by the policy rule set applied to them. [0111] FIG. 19 is a more detailed schematic block diagram of the policy engine 510 according to one embodiment of the invention. The policy engine 510 includes a policy request table 602 that acts as a queue for all the policy decision requests. In this regard, the portion of the packet matching the information stored in the stream table 506 is presented to the policy engine 510 in the form of a policy request. The policy request is then queued in the policy request table 602. [0112] A resource engine 604 maintains an up-to-date mapping of resource group names to member mappings. A policy rules database buffer 608 stores a current policy rule set to be applied by the policy engine 510. The policy rules stored in the buffer 608 are preferably in the original group-based rule specification format. Thus, the buffer 608 stores a rule created for a group in its group-based form instead of instantiating a rule for each member of the group.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	[0113] A decision engine 606 includes logic to serve the incoming policy decision requests in the policy request table 602 by matching it against the policy rule set in the policy rules database buffer 608 based on the actual membership information obtained from the resource engine 604. The relevant group-based rule matching the traffic is then identified and decision bits in the stream table set for enforcing the corresponding actions. The decision bits thus constitute the set of actions to be performed on the packets of the stream. All packets matching the streams are then processed based on these decision bits. The decision engine may also specify an access control list (ACL) including a set of rules that allow/deny traffic, a DiffServ standard for providing a quality of service level to the traffic, and/or VPN implementation information.
	[0133] The policy server 122 preferably stores the policy management information for all the policy enforcers in the policy server database 130. This information is organized in the databases 130 as one or more DNs with corresponding attributes. Appropriate portions of the policy server database are then copied to the policy enforcer databases 132, 134.
	[Cl. 1] In a system including a first edge device managing policies for a first network according to first policy settings and a second edge device managing policies for a second network according to second policy settings, the system further including a central policy server in communication with the first and second edge devices configured to define the first and second policy settings and manage the first and second edge devices from a single location, each edge device comprising: a classification engine for determining a protocol associated with an incoming packet; a policy engine for making a forwarding decision for the packet based on policy settings associated with the packet; and a packet forwarding module for forwarding the packet based on the policy settings.
	***See* Jain Figs. 1, 3, 11, 18, 19**
	To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[1d] provide the one or more traffic inspection provisioning instructions to the network traffic inspection system; and	Jain discloses providing the one or more traffic inspection provisioning instructions to the network traffic inspection system. *See, e.g.*:

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	[0007] The present invention is directed to a unified policy management system where various policies, namely, the set of rules and instructions that determine the network=s operation, may be established and enforced from a single site. According to one embodiment of the invention, the system includes a first edge device associated with a first network having a first set of resources that is configured to manage the policies for the first network according to the policy settings stored in a first database. The system also includes a second edge device associated with a second network having a second set of resources that is configured to manage the policies for the second network according to the policy settings stored in a second database. The first and second edge devices act as policy enforcers for their respective networks. The policies being enforced may include firewall policies, VPN policies, and the like. [0008] The system further includes a central policy server in communication with the first and second edge devices. The policy server is configured to define the first and second policy settings and manage the first and second edge devices from a single location. Thus, a network administrator need not multiply his or her efforts and associated expenditures in configuring and managing the policy enforcers individually. [0017] The functionalities of the policy enforcers in enforcing the policies for their respective networks may also be partitioned for effective hardware implementation. According to one embodiment of the invention, each edge device preferably includes a plurality of modules including a classification engine, a policy engine, and a packet forwarding engine. The classification engine determines a protocol associated with an incoming packet. The policy engine makes a forwarding decision for the packet based on policy settings associated with the packet. The packet forwarding module then forwards the packet based on the policy settings. [0030] Local network 102 includes a policy server 122 for defining and managing network services and policies for the organization. The network policies are a set of rules and instructions that determine the network=s operation, such as firewall, VPN, bandwidth, and administration policies. The firewall policies decide the network traffic that is to be allowed to flow from the public Internet 108 into the local networks 102, 104, and the traffic that is to be blocked. The bandwidth policies determine the kind of bandwidth that is to be allocated to the traffic flowing through the local networks. The VPN policies determine the rules for implementing multiple site connectivity across the local networks. The administration policies decide the users that have access to administrative functions, the type of administrative functions allocated to these users, and the policy enforcers 124, 126 on which these users may exercise such administrative functions. The firewall, VPN, bandwidth,

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	and administration policies for the entire organization are preferably stored in a policy server database 130 maintained by the policy server 122. **[0031]** Each local network 102, 104 also includes an edge device, referred to as a policy enforcer 124, 126, for controlling access to the network. Each policy enforcer 124, 126 manages the network policies and services for the users and resources of their respective local networks 102, 104, as permitted by the policy server 122. Respective portions of the policy server database 130 are copied to the policy enforcer databases 132, 134 for allowing the policy enforcers to manage the network policies and services for the local networks 102, 104. **[0033]** According to one embodiment of the invention, a policy object 222 includes a bandwidth policy 224, firewall policy 226, administration policy 228, and VPN policy 230. The VPN policy 230 defines a security policy for the member networks and includes one or more VPN clouds 232. Each VPN cloud 232 is an individual VPN or a group of VPNs defining a security policy group which includes a list of sites 234 and users 236 who can communicate with each other. A site is preferably a set of hosts/networks physically located behind one of the policy enforcers 124, 126. In other words, a site is a definition of a network which includes the policy enforcer that is associated with it. The policy enforcers for the sites act as VPN tunnel endpoints once the hosts under the sites start communicating. These communications are governed by a set of rules 238 configured for each VPN cloud. The rules 238 may govern, among other things, VPN access permissions and security features such as the level of encryption and authentication used for the connectivity at the network layer. **[0045]** FIG. 3 is a more detailed schematic block diagram of the policy server 122 according to one embodiment of the invention. The policy server 122 preferably includes a management module 302 that allows centralized control over the policy enforcers 124, 126 from a single console. The policy server 122 further includes a log collecting and archiving module 304 and a policy server reports module 316. The log collecting and archiving module 304 collects information about the status and usage of resources from the policy enforcers 124, 126 as well as from the management module 302, and stores them in an archive database 318. The policy server reports module 316 uses the collected logs and archives to generate reports in an organized report format. **[0047]** The centralized management sub-module 306 enables a network administrator to install and manage individual policy enforcers from a central location. The network administrator preferably uses a web-based graphical user interface to define the policy enforcer's network configuration and monitor various aspects of the device, such as device health, device alarms, VPN connection status, and the like.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

[0048] The policy management sub-module 308 provides the network administrator with the ability to create policies that span multiple functional aspects of the policy enforcer (e.g. firewall, bandwidth management, and virtual private networks), multiple resources (e.g. users, hosts, services and time), and multiple policy enforcers.
[0057] Referring again to FIG. 4, the centralized management sub-module 306 also includes a global monitor user interface 402 and a data collector program 412, respectively displaying and collecting the health and status of all the policy enforcers managed by the policy server 122. The data collector program 412 receives health and status information from each of the up-and-running policy enforcers it manages, and passes the relevant information to the global monitor user interface. A health agent running as a daemon in each of the policy enforcers being monitored periodically collects data from the device and analyzes its health status. The collected data is then transferred to the policy server 122 when requested by the data collector program 412.
[0059] Referring again to FIG. 3, the policy management sub-module 308 allows for policy management of the policy enforcers 124, 126. As discussed above, all policy management functions are implemented in terms of resource objects stored in the policy databases 130, 132, 134 including users, devices, hosts, services, and time. Preferably, all resources are associated with default policy settings selected by the administrator during the installation process. The network administrator views, adds, and modifies the policies centrally via a graphical user interface provided by the policy management sub-module 308. This allows for a policy-centric management model where the administrator is given the impression that a single logical server provides the firewall, bandwidth management, and VPN services across the enterprise. The fact that the policy is enforced on individual policy enforcers in different locations is transparent to the administrator.
[0070] According to one embodiment of the invention, each firewall policy includes a policy identifier (ID) attribute 724 for identifying a particular policy rule in the list of policies. An order number attribute 726 for the policy rule indicates the sequence in which the policy is to be applied. In this regard, the policy enforcer 124, 126 for the local network takes one rule at a time, in sequence, compares it against the network traffic, and preferably applies the first rule that matches the network traffic.
[0071] Each firewall policy also includes a description attribute 728 for describing the firewall policy to be applied. For instance, the description may indicate that the policy allows spam blocking, URL blocking, VPN key management, and the like. An action flag attribute 730 indicates whether traffic is

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

| | to be allowed or denied for the indicated policy. An active flag attribute 732 indicates whether the policy has been activated or de-activated. Thus, the network administrator may create a policy and activate it at a later time. A policy that has been de-activated preferably has no effect on the network traffic.

[0072] Each firewall policy further includes a user attribute 734, source attribute 736, service attribute 738, destination attribute (not shown), and time attribute (not shown). Each of these attributes is preferably represented by a group name or a resource name. The name acts as a pointer to an entry in the group root object 202 or resource root object of the LDAP database 130, 132, or 134.

[0078] Referring again to FIG. 8, selection of the bandwidth tab 720c allows the display, addition, and modification of various bandwidth policies determining the kind of bandwidth to be allocated to a traffic flowing through a particular policy enforcer. Different bandwidths may be specified for different users, hosts, and services.

[0107] FIG. 18 is a schematic block diagram of the policy enforcer 124, 126 illustrating the partitioning of the various functionalities according to one embodiment of the invention. The policy enforcer includes an Internet protocol security (IPSec) engine 502 for performing security and authentication functions in implementing, for instance, virtual private networks. A stream table 506 assembles the packets passing through the policy enforcer into streams. A protocol classification engine 508 decodes the protocols used in forwarding the packets. A policy engine 510 enforces policies for the packets based on the policy settings stored in the policy database 132, 134. A packet forwarding module 504 receives packets from the public Internet via the router 110 and buffers, forwards, or drops the packets based on the policies being enforced. A bandwidth management module 514 provides bandwidth shaping services to the packets being forwarded based on the bandwidth settings stored in the policy database 132, 134.

[0108] In practice, an incoming packet is matched against the stream table 506 for determining if a matching entry already exists in the table. If not, a new entry is added. The stream table preferably includes enough portions of the packet to uniquely identify a stream. For example, in enforcing policies on IP layer three through layer four traffic, the stream table may store a source IP, destination IP, source port, destination port, and protocol number of the incoming packet.

[0109] The protocol classification engine 508 takes the new stream and obtains a detailed protocol decode for the stream. The policy engine 510 is then queried for the policy rules to be applied to the |

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

stream. Based on the policy rules returned by the policy engine 510, the packet forwarding module 504, IPSec engine 502, and/or the bandwidth management module 514 process the streams accordingly. The processing may be recursive until the packets in the stream have had all the actions specified by the policy rule set applied to them.

[0111] FIG. 19 is a more detailed schematic block diagram of the policy engine 510 according to one embodiment of the invention. The policy engine 510 includes a policy request table 602 that acts as a queue for all the policy decision requests. In this regard, the portion of the packet matching the information stored in the stream table 506 is presented to the policy engine 510 in the form of a policy request. The policy request is then queued in the policy request table 602.

[0112] A resource engine 604 maintains an up-to-date mapping of resource group names to member mappings. A policy rules database buffer 608 stores a current policy rule set to be applied by the policy engine 510. The policy rules stored in the buffer 608 are preferably in the original group-based rule specification format. Thus, the buffer 608 stores a rule created for a group in its group-based form instead of instantiating a rule for each member of the group.

[0113] A decision engine 606 includes logic to serve the incoming policy decision requests in the policy request table 602 by matching it against the policy rule set in the policy rules database buffer 608 based on the actual membership information obtained from the resource engine 604. The relevant group-based rule matching the traffic is then identified and decision bits in the stream table set for enforcing the corresponding actions. The decision bits thus constitute the set of actions to be performed on the packets of the stream. All packets matching the streams are then processed based on these decision bits. The decision engine may also specify an access control list (ACL) including a set of rules that allow/deny traffic, a DiffServ standard for providing a quality of service level to the traffic, and/or VPN implementation information.

[0133] The policy server 122 preferably stores the policy management information for all the policy enforcers in the policy server database 130. This information is organized in the databases 130 as one or more DNs with corresponding attributes. Appropriate portions of the policy server database are then copied to the policy enforcer databases 132, 134.

[Cl. 1] In a system including a first edge device managing policies for a first network according to first policy settings and a second edge device managing policies for a second network according to second policy settings, the system further including a central policy server in communication with the

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	first and second edge devices configured to define the first and second policy settings and manage the first and second edge devices from a single location, each edge device comprising: a classification engine for determining a protocol associated with an incoming packet; a policy engine for making a forwarding decision for the packet based on policy settings associated with the packet; and a packet forwarding module for forwarding the packet based on the policy settings. *See* **Jain Figs. 1, 3, 11, 18, 19** To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[1e] provide the one or more policy enforcement provisioning instructions to the network policy enforcement system.	Jain discloses providing the one or more policy enforcement provisioning instructions to the network policy enforcement system. *See, e.g.*: **[0007]** The present invention is directed to a unified policy management system where various policies, namely, the set of rules and instructions that determine the network=s operation, may be established and enforced from a single site. According to one embodiment of the invention, the system includes a first edge device associated with a first network having a first set of resources that is configured to manage the policies for the first network according to the policy settings stored in a first database. The system also includes a second edge device associated with a second network having a second set of resources that is configured to manage the policies for the second network according to the policy settings stored in a second database. The first and second edge devices act as policy enforcers for their respective networks. The policies being enforced may include firewall policies, VPN policies, and the like. **[0008]** The system further includes a central policy server in communication with the first and second edge devices. The policy server is configured to define the first and second policy settings and manage the first and second edge devices from a single location. Thus, a network administrator need not multiply his or her efforts and associated expenditures in configuring and managing the policy enforcers individually.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

| | [0017] The functionalities of the policy enforcers in enforcing the policies for their respective networks may also be partitioned for effective hardware implementation. According to one embodiment of the invention, each edge device preferably includes a plurality of modules including a classification engine, a policy engine, and a packet forwarding engine. The classification engine determines a protocol associated with an incoming packet. The policy engine makes a forwarding decision for the packet based on policy settings associated with the packet. The packet forwarding module then forwards the packet based on the policy settings.

[0030] Local network 102 includes a policy server 122 for defining and managing network services and policies for the organization. The network policies are a set of rules and instructions that determine the network=s operation, such as firewall, VPN, bandwidth, and administration policies. The firewall policies decide the network traffic that is to be allowed to flow from the public Internet 108 into the local networks 102, 104, and the traffic that is to be blocked. The bandwidth policies determine the kind of bandwidth that is to be allocated to the traffic flowing through the local networks. The VPN policies determine the rules for implementing multiple site connectivity across the local networks. The administration policies decide the users that have access to administrative functions, the type of administrative functions allocated to these users, and the policy enforcers 124, 126 on which these users may exercise such administrative functions. The firewall, VPN, bandwidth, and administration policies for the entire organization are preferably stored in a policy server database 130 maintained by the policy server 122.

[0031] Each local network 102, 104 also includes an edge device, referred to as a policy enforcer 124, 126, for controlling access to the network. Each policy enforcer 124, 126 manages the network policies and services for the users and resources of their respective local networks 102, 104, as permitted by the policy server 122. Respective portions of the policy server database 130 are copied to the policy enforcer databases 132, 134 for allowing the policy enforcers to manage the network policies and services for the local networks 102, 104.

[0033] According to one embodiment of the invention, a policy object 222 includes a bandwidth policy 224, firewall policy 226, administration policy 228, and VPN policy 230. The VPN policy 230 defines a security policy for the member networks and includes one or more VPN clouds 232. Each VPN cloud 232 is an individual VPN or a group of VPNs defining a security policy group which includes a list of sites 234 and users 236 who can communicate with each other. A site is preferably a set of hosts/networks physically located behind one of the policy enforcers 124, 126. In other words, a site is a definition of a network which includes the policy enforcer that is associated with it. The policy enforcers for the sites act as VPN tunnel endpoints once the hosts under the sites start |

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

| | communicating. These communications are governed by a set of rules 238 configured for each VPN cloud. The rules 238 may govern, among other things, VPN access permissions and security features such as the level of encryption and authentication used for the connectivity at the network layer. |
| | |

communicating. These communications are governed by a set of rules 238 configured for each VPN cloud. The rules 238 may govern, among other things, VPN access permissions and security features such as the level of encryption and authentication used for the connectivity at the network layer.

[0045] FIG. 3 is a more detailed schematic block diagram of the policy server 122 according to one embodiment of the invention. The policy server 122 preferably includes a management module 302 that allows centralized control over the policy enforcers 124, 126 from a single console. The policy server 122 further includes a log collecting and archiving module 304 and a policy server reports module 316. The log collecting and archiving module 304 collects information about the status and usage of resources from the policy enforcers 124, 126 as well as from the management module 302, and stores them in an archive database 318. The policy server reports module 316 uses the collected logs and archives to generate reports in an organized report format.

[0047] The centralized management sub-module 306 enables a network administrator to install and manage individual policy enforcers from a central location. The network administrator preferably uses a web-based graphical user interface to define the policy enforcer's network configuration and monitor various aspects of the device, such as device health, device alarms, VPN connection status, and the like.

[0048] The policy management sub-module 308 provides the network administrator with the ability to create policies that span multiple functional aspects of the policy enforcer (e.g. firewall, bandwidth management, and virtual private networks), multiple resources (e.g. users, hosts, services and time), and multiple policy enforcers.

[0057] Referring again to FIG. 4, the centralized management sub-module 306 also includes a global monitor user interface 402 and a data collector program 412, respectively displaying and collecting the health and status of all the policy enforcers managed by the policy server 122. The data collector program 412 receives health and status information from each of the up-and-running policy enforcers it manages, and passes the relevant information to the global monitor user interface. A health agent running as a daemon in each of the policy enforcers being monitored periodically collects data from the device and analyzes its health status. The collected data is then transferred to the policy server 122 when requested by the data collector program 412.

[0059] Referring again to FIG. 3, the policy management sub-module 308 allows for policy management of the policy enforcers 124, 126. As discussed above, all policy management functions are implemented in terms of resource objects stored in the policy databases 130, 132, 134 including

28

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

users, devices, hosts, services, and time. Preferably, all resources are associated with default policy settings selected by the administrator during the installation process. The network administrator views, adds, and modifies the policies centrally via a graphical user interface provided by the policy management sub-module 308. This allows for a policy-centric management model where the administrator is given the impression that a single logical server provides the firewall, bandwidth management, and VPN services across the enterprise. The fact that the policy is enforced on individual policy enforcers in different locations is transparent to the administrator.

[0070] According to one embodiment of the invention, each firewall policy includes a policy identifier (ID) attribute 724 for identifying a particular policy rule in the list of policies. An order number attribute 726 for the policy rule indicates the sequence in which the policy is to be applied. In this regard, the policy enforcer 124, 126 for the local network takes one rule at a time, in sequence, compares it against the network traffic, and preferably applies the first rule that matches the network traffic.

[0071] Each firewall policy also includes a description attribute 728 for describing the firewall policy to be applied. For instance, the description may indicate that the policy allows spam blocking, URL blocking, VPN key management, and the like. An action flag attribute 730 indicates whether traffic is to be allowed or denied for the indicated policy. An active flag attribute 732 indicates whether the policy has been activated or de-activated. Thus, the network administrator may create a policy and activate it at a later time. A policy that has been de-activated preferably has no effect on the network traffic.

[0072] Each firewall policy further includes a user attribute 734, source attribute 736, service attribute 738, destination attribute (not shown), and time attribute (not shown). Each of these attributes is preferably represented by a group name or a resource name. The name acts as a pointer to an entry in the group root object 202 or resource root object of the LDAP database 130, 132, or 134.

[0078] Referring again to FIG. 8, selection of the bandwidth tab 720c allows the display, addition, and modification of various bandwidth policies determining the kind of bandwidth to be allocated to a traffic flowing through a particular policy enforcer. Different bandwidths may be specified for different users, hosts, and services.

[0107] FIG. 18 is a schematic block diagram of the policy enforcer 124, 126 illustrating the partitioning of the various functionalities according to one embodiment of the invention. The policy

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

enforcer includes an Internet protocol security (IPSec) engine 502 for performing security and authentication functions in implementing, for instance, virtual private networks. A stream table 506 assembles the packets passing through the policy enforcer into streams. A protocol classification engine 508 decodes the protocols used in forwarding the packets. A policy engine 510 enforces policies for the packets based on the policy settings stored in the policy database 132, 134. A packet forwarding module 504 receives packets from the public Internet via the router 110 and buffers, forwards, or drops the packets based on the policies being enforced. A bandwidth management module 514 provides bandwidth shaping services to the packets being forwarded based on the bandwidth settings stored in the policy database 132, 134.

[0108] In practice, an incoming packet is matched against the stream table 506 for determining if a matching entry already exists in the table. If not, a new entry is added. The stream table preferably includes enough portions of the packet to uniquely identify a stream. For example, in enforcing policies on IP layer three through layer four traffic, the stream table may store a source IP, destination IP, source port, destination port, and protocol number of the incoming packet.

[0109] The protocol classification engine 508 takes the new stream and obtains a detailed protocol decode for the stream. The policy engine 510 is then queried for the policy rules to be applied to the stream. Based on the policy rules returned by the policy engine 510, the packet forwarding module 504, IPSec engine 502, and/or the bandwidth management module 514 process the streams accordingly. The processing may be recursive until the packets in the stream have had all the actions specified by the policy rule set applied to them.

[0111] FIG. 19 is a more detailed schematic block diagram of the policy engine 510 according to one embodiment of the invention. The policy engine 510 includes a policy request table 602 that acts as a queue for all the policy decision requests. In this regard, the portion of the packet matching the information stored in the stream table 506 is presented to the policy engine 510 in the form of a policy request. The policy request is then queued in the policy request table 602.

[0112] A resource engine 604 maintains an up-to-date mapping of resource group names to member mappings. A policy rules database buffer 608 stores a current policy rule set to be applied by the policy engine 510. The policy rules stored in the buffer 608 are preferably in the original group-based rule specification format. Thus, the buffer 608 stores a rule created for a group in its group-based form instead of instantiating a rule for each member of the group.

Case 2:23-cv-00352-JRG-RSP   Document 77-6   Filed 08/21/24   Page 32 of 61 PageID #:
5878
Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	[0113] A decision engine 606 includes logic to serve the incoming policy decision requests in the policy request table 602 by matching it against the policy rule set in the policy rules database buffer 608 based on the actual membership information obtained from the resource engine 604. The relevant group-based rule matching the traffic is then identified and decision bits in the stream table set for enforcing the corresponding actions. The decision bits thus constitute the set of actions to be performed on the packets of the stream. All packets matching the streams are then processed based on these decision bits. The decision engine may also specify an access control list (ACL) including a set of rules that allow/deny traffic, a DiffServ standard for providing a quality of service level to the traffic, and/or VPN implementation information. **[0133]** The policy server 122 preferably stores the policy management information for all the policy enforcers in the policy server database 130. This information is organized in the databases 130 as one or more DNs with corresponding attributes. Appropriate portions of the policy server database are then copied to the policy enforcer databases 132, 134. **[Cl. 1]** In a system including a first edge device managing policies for a first network according to first policy settings and a second edge device managing policies for a second network according to second policy settings, the system further including a central policy server in communication with the first and second edge devices configured to define the first and second policy settings and manage the first and second edge devices from a single location, each edge device comprising: a classification engine for determining a protocol associated with an incoming packet; a policy engine for making a forwarding decision for the packet based on policy settings associated with the packet; and a packet forwarding module for forwarding the packet based on the policy settings. ***See* Jain Figs. 1, 3, 11, 18, 19** To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[2] The network service plan provisioning system of claim 1, wherein process the first service plan component	Jain discloses the network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises order traffic inspection comparison operations in the one or more traffic inspection provisioning instructions such that the one or more traffic inspection provisioning instructions direct the network traffic inspection system to determine whether the traffic event possesses the characteristic that matches the first traffic classification filter before determining whether the traffic event possesses the characteristic that matches the second traffic classification filter.	second traffic classification filter comprises order traffic inspection comparison operations in the one or more traffic inspection provisioning instructions such that the one or more traffic inspection provisioning instructions direct the network traffic inspection system to determine whether the traffic event possesses the characteristic that matches the first traffic classification filter before determining whether the traffic event possesses the characteristic that matches the second traffic classification filter. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 2. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[3] The network service plan provisioning system of claim 2, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter further comprises include in the network provisioning instruction set one or more instructions directing the network traffic inspection system to determine whether the traffic event possesses the characteristic that matches the second	Jain discloses the network service plan provisioning system of claim 2, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter further comprises include in the network provisioning instruction set one or more instructions directing the network traffic inspection system to determine whether the traffic event possesses the characteristic that matches the second traffic classification filter only if the traffic event does not possess the characteristic that matches the first traffic classification filter. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 3. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

traffic classification filter only if the traffic event does not possess the characteristic that matches the first traffic classification filter.	
[4] The network service plan provisioning system of claim 2, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter further comprises include in the network provisioning instruction set one or more instructions directing the network traffic inspection system to determine whether the traffic event also possesses the characteristic that matches the second traffic classification filter if the traffic event possesses the characteristic that matches the first traffic classification filter.	Jain discloses the network service plan provisioning system of claim 2, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter further comprises include in the network provisioning instruction set one or more instructions directing the network traffic inspection system to determine whether the traffic event also possesses the characteristic that matches the second traffic classification filter if the traffic event possesses the characteristic that matches the first traffic classification filter. *See supra* claims 1 and 2. In addition, Jain anticipates and/or renders obvious claim 4. *See supra* claims 1 and 2. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[5p] The network service plan provisioning system of claim 1, further comprising:	Jain discloses the network service plan provisioning system of claim 1. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 5. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[5a] a policy enforcement priority rule datastore including a policy	Jain discloses a policy enforcement priority rule datastore including a policy enforcement priority rule for determining whether the traffic event possesses the characteristic that matches the first traffic

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

enforcement priority rule for determining whether the traffic event possesses the characteristic that matches the first traffic classification filter before determining whether the traffic event possesses the characteristic that matches the second traffic classification filter,	classification filter before determining whether the traffic event possesses the characteristic that matches the second traffic classification filter. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 5. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[5b] and wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises include the policy enforcement priority rule in the network provisioning instruction set.	Jain discloses and wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises include the policy enforcement priority rule in the network provisioning instruction set. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 5. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[6] The network service plan provisioning system of claim 5, wherein the policy enforcement priority rule comprises a priority order for a plurality of traffic classification filters, the plurality of traffic classification filters including the first traffic classification filter and the second traffic classification filter.	Jain discloses the network service plan provisioning system of claim 5, wherein the policy enforcement priority rule comprises a priority order for a plurality of traffic classification filters, the plurality of traffic classification filters including the first traffic classification filter and the second traffic classification filter. *See supra* claims 1 and 5. In addition, Jain anticipates and/or renders obvious claim 6. *See supra* claims 1 and 5. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

[7] The network service plan provisioning system of claim 5, wherein the policy enforcement priority rule comprises a priority specification for one or both of the first service plan component and the second service plan component.	Jain discloses the network service plan provisioning system of claim 5, wherein the policy enforcement priority rule comprises a priority specification for one or both of the first service plan component and the second service plan component. *See supra* claims 1 and 5. In addition, Jain anticipates and/or renders obvious claim 7. *See supra* claims 1 and 5. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[8] The network service plan provisioning system of claim 1, wherein at least one of the one or more policies is dependent on a network state.	Jain discloses the network service plan provisioning system of claim 1, wherein at least one of the one or more policies is dependent on a network state. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 8. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[9] The network service plan provisioning system of claim 8, wherein the network state comprises a congestion state of the wireless access network, a network location, a type of the wireless access network, whether the wireless access network is a roaming network, a routing identifier associated with the wireless access network, or a combination of these.	Jain discloses the network service plan provisioning system of claim 8, wherein the network state comprises a congestion state of the wireless access network, a network location, a type of the wireless access network, whether the wireless access network is a roaming network, a routing identifier associated with the wireless access network, or a combination of these. *See supra* claims 1 and 8. In addition, Jain anticipates and/or renders obvious claim 9. *See supra* claims 1 and 8. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

[10] The network service plan provisioning system of claim 9, wherein the congestion state is based on a time of day, a measure of network congestion, a measure of a delay, a measure of a jitter, a packet error rate, or a combination of these.	Jain discloses the network service plan provisioning system of claim 9, wherein the congestion state is based on a time of day, a measure of network congestion, a measure of a delay, a measure of a jitter, a packet error rate, or a combination of these. *See supra* claims 1, 8, and 9. In addition, Jain anticipates and/or renders obvious claim 10. *See supra* claims 1, 8, and 9. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[11] The network service plan provisioning system of claim 5, wherein the one or more network elements are further configured to provide a user interface for a service plan design environment that provides for entering the policy enforcement priority rule in the design environment by entering a priority assignment for the first service plan component, entering a priority assignment for the second service plan component, positioning the first and second service plan components in a priority ordering, defining the first or second service plan component as belonging to a service type that has an implied or literal ordering, or a combination of these.	Jain discloses the network service plan provisioning system of claim 5, wherein the one or more network elements are further configured to provide a user interface for a service plan design environment that provides for entering the policy enforcement priority rule in the design environment by entering a priority assignment for the first service plan component, entering a priority assignment for the second service plan component, positioning the first and second service plan components in a priority ordering, defining the first or second service plan component as belonging to a service type that has an implied or literal ordering, or a combination of these. *See supra* claims 1 and 5. In addition, Jain anticipates and/or renders obvious claim 11. *See supra* claims 1 and 5. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[12] The network service plan provisioning system of claim 1, wherein the information specifying the first	Jain discloses the network service plan provisioning system of claim 1, wherein the information specifying the first traffic classification filter comprises an inspection criterion selected from a group of inspection criteria consisting of: specific device application, a specific network destination, a

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

traffic classification filter comprises an inspection criterion selected from a group of inspection criteria consisting of: specific device application, a specific network destination, a specific network source, a specific traffic type, a specific content type, a specific traffic protocol, and a combination of two or more of the inspection criteria.	specific network source, a specific traffic type, a specific content type, a specific traffic protocol, and a combination of two or more of the inspection criteria. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 12. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[13] The network service plan provisioning system of claim 1, wherein the first or second policy enforcement action is an action selected from a group of actions consisting of: apply a traffic control policy; apply a service usage accounting, charging, or billing policy; apply a service notification policy; and a combination of two or more of the actions.	Jain discloses the network service plan provisioning system of claim 1, wherein the first or second policy enforcement action is an action selected from a group of actions consisting of: apply a traffic control policy; apply a service usage accounting, charging, or billing policy; apply a service notification policy; and a combination of two or more of the actions. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 13. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[15] The network service plan provisioning system of claim 1, wherein the one or more network elements are further configured to include in the network provisioning instruction set an instruction to assist in enforcing a classification-based charging policy, wherein the classification is selected from the group of classification categories consisting of: application, destination, network, time of day, congestion state, quality of service,	Jain discloses the network service plan provisioning system of claim 1, wherein the one or more network elements are further configured to include in the network provisioning instruction set an instruction to assist in enforcing a classification-based charging policy, wherein the classification is selected from the group of classification categories consisting of: application, destination, network, time of day, congestion state, quality of service, content type, and a combination of two or more of the classification categories. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 15. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it

37

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

content type, and a combination of two or more of the classification categories.	would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[16] The network service plan provisioning system of claim 1, wherein the one or more network elements are further configured to include in the network provisioning instruction set an instruction to assist in presenting a service buy page notification with an actionable response.	Jain discloses the network service plan provisioning system of claim 1, wherein the one or more network elements are further configured to include in the network provisioning instruction set an instruction to assist in presenting a service buy page notification with an actionable response. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 16. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[21] The network service plan provisioning system of claim 1, wherein the one or more network elements are further configured to facilitate reuse of the first service plan component, the second service plan component, the first traffic classification filter, the second traffic classification filter, the first policy enforcement action, or the second policy enforcement action in a plurality of service plans by storing the first service plan component, the second service plan component, the first traffic classification filter, the second traffic classification filter, the first policy enforcement action, and the second policy enforcement action as one or more objects in a catalog.	Jain discloses the network service plan provisioning system of claim 1, wherein the one or more network elements are further configured to facilitate reuse of the first service plan component, the second service plan component, the first traffic classification filter, the second traffic classification filter, the first policy enforcement action, or the second policy enforcement action in a plurality of service plans by storing the first service plan component, the second service plan component, the first traffic classification filter, the second traffic classification filter, the first policy enforcement action, and the second policy enforcement action as one or more objects in a catalog. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 21. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

[22] The network service plan provisioning system of claim 1, wherein the first service plan component further comprises an additional policy enforcement action to augment the first policy enforcement action, and wherein the second service plan component further comprises the additional policy enforcement action to augment the second policy enforcement action.	Jain discloses the network service plan provisioning system of claim 1, wherein the first service plan component further comprises an additional policy enforcement action to augment the first policy enforcement action, and wherein the second service plan component further comprises the additional policy enforcement action to augment the second policy enforcement action. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 22. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[23] The network service plan provisioning system of claim 1, wherein the first service plan component further comprises an additional policy enforcement action to over-ride the first policy enforcement action, and wherein the second service plan component further comprises the additional policy enforcement action to over-ride the second policy enforcement action.	Jain discloses the network service plan provisioning system of claim 1, wherein the first service plan component further comprises an additional policy enforcement action to over-ride the first policy enforcement action, and wherein the second service plan component further comprises the additional policy enforcement action to over-ride the second policy enforcement action. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 23. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[28] The network service plan provisioning system of claim 1, wherein the one or more network elements are further configured to obtain service plan parameters for multiple service plans, combine one or more service policies for the multiple service plans into one composite-plan policy set, and provision the network policy enforcement system to enforce the	Jain discloses the network service plan provisioning system of claim 1, wherein the one or more network elements are further configured to obtain service plan parameters for multiple service plans, combine one or more service policies for the multiple service plans into one composite-plan policy set, and provision the network policy enforcement system to enforce the composite policies for the multiple service plans. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 28. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

composite policies for the multiple service plans.	would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[30] The network service plan provisioning system of claim 1, wherein the first service plan component is associated with a first priority, and wherein the second service plan component is associated with a second priority, the second priority being lower than the first priority, and wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises include in the network provisioning instruction set one or more first instructions directing the network traffic inspection system to determine whether the traffic event possesses the characteristic that matches the first traffic classification filter and to determine whether the traffic event possesses the characteristic that matches the second traffic classification filter, and one or more second instructions directing the network policy enforcement system to enforce the first network policy enforcement action when the traffic event possesses both the characteristic that matches the first traffic classification filter and the	Jain discloses the network service plan provisioning system of claim 1, wherein the first service plan component is associated with a first priority, and wherein the second service plan component is associated with a second priority, the second priority being lower than the first priority, and wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises include in the network provisioning instruction set one or more first instructions directing the network traffic inspection system to determine whether the traffic event possesses the characteristic that matches the first traffic classification filter and to determine whether the traffic event possesses the characteristic that matches the second traffic classification filter, and one or more second instructions directing the network policy enforcement system to enforce the first network policy enforcement action when the traffic event possesses both the characteristic that matches the first traffic classification filter and the characteristic that matches the second traffic classification filter. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 30. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

characteristic that matches the second traffic classification filter.	
[31] The network service plan provisioning system of claim 1, wherein the first service plan component is associated with a first priority, and wherein the second service plan component is associated with a second priority, the second priority being lower than the first priority, and wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises include in the network provisioning instruction set one or more first instructions directing the network traffic inspection system to determine whether the traffic event possesses the characteristic that matches the first traffic classification filter, and one or more second instructions directing the network policy enforcement system to enforce only the first network policy enforcement action when the traffic event possesses the characteristic that matches the first traffic classification filter.	Jain discloses the network service plan provisioning system of claim 1, wherein the first service plan component is associated with a first priority, and wherein the second service plan component is associated with a second priority, the second priority being lower than the first priority, and wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises include in the network provisioning instruction set one or more first instructions directing the network traffic inspection system to determine whether the traffic event possesses the characteristic that matches the first traffic classification filter, and one or more second instructions directing the network policy enforcement system to enforce only the first network policy enforcement action when the traffic event possesses the characteristic that matches the first traffic classification filter. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 31. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

| [32] The network service plan provisioning system of claim 1, wherein the first service plan component is associated with a first priority, and wherein the second service plan component is associated with a second priority, the second priority being lower than the first priority, and wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises include in the network provisioning instruction set one or more first instructions directing the network traffic inspection system to determine whether the traffic event possesses the characteristic that matches the first traffic classification filter and to determine whether the traffic event possesses the characteristic that matches the second traffic classification filter, and one or more second instructions directing the network policy enforcement system to enforce the first network policy enforcement action and the second network policy enforcement action when the traffic event possesses both the characteristic that matches the first traffic classification filter and the characteristic that matches the second traffic classification filter. | Jain discloses the network service plan provisioning system of claim 1, wherein the first service plan component is associated with a first priority, and wherein the second service plan component is associated with a second priority, the second priority being lower than the first priority, and wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises include in the network provisioning instruction set one or more first instructions directing the network traffic inspection system to determine whether the traffic event possesses the characteristic that matches the first traffic classification filter and to determine whether the traffic event possesses the characteristic that matches the second traffic classification filter, and one or more second instructions directing the network policy enforcement system to enforce the first network policy enforcement action and the second network policy enforcement action when the traffic event possesses both the characteristic that matches the first traffic classification filter and the characteristic that matches the second traffic classification filter. *See supra* claim 1.

In addition, Jain anticipates and/or renders obvious claim 32. *See supra* claim 1.

To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached. |

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

[33] The network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises order one or more first instructions associated with the first traffic classification filter and one or more second instructions associated with the second traffic classification filter so that the first traffic classification filter is applied to the traffic event before the second traffic classification filter is applied to the traffic event.	Jain discloses the network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises order one or more first instructions associated with the first traffic classification filter and one or more second instructions associated with the second traffic classification filter so that the first traffic classification filter is applied to the traffic event before the second traffic classification filter is applied to the traffic event. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 33. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[35] The network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises apply an explicit priority rule.	Jain discloses the network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises apply an explicit priority rule. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 35. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[36] The network service plan provisioning system of claim 1, wherein	Jain discloses the network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises configure the one or more traffic inspection provisioning instructions so that the network traffic inspection system determines whether the traffic event possesses the characteristic that matches the first traffic classification filter before determining whether the traffic event possesses the characteristic that matches the second traffic classification filter.	instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises configure the one or more traffic inspection provisioning instructions so that the network traffic inspection system determines whether the traffic event possesses the characteristic that matches the first traffic classification filter before determining whether the traffic event possesses the characteristic that matches the second traffic classification filter. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 36. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[37] The network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises configure the one or more policy enforcement provisioning instructions so that the network policy enforcement system applies the first policy enforcement action before applying the second policy enforcement action.	Jain discloses the network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises configure the one or more policy enforcement provisioning instructions so that the network policy enforcement system applies the first policy enforcement action before applying the second policy enforcement action. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 37. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

[38] The network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises configure the one or more traffic inspection provisioning instructions so that when the traffic event possesses the characteristic that matches the first traffic classification filter, the network policy enforcement system applies the first policy enforcement action, and the network traffic inspection system does not determine whether the traffic event possesses the characteristic that matches the second traffic classification filter.	Jain discloses the network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises configure the one or more traffic inspection provisioning instructions so that when the traffic event possesses the characteristic that matches the first traffic classification filter, the network policy enforcement system applies the first policy enforcement action, and the network traffic inspection system does not determine whether the traffic event possesses the characteristic that matches the second traffic classification filter. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 38. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[39] The network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises configure the network provisioning instruction set so that when the traffic event possesses the characteristic that matches the first traffic classification filter and the characteristic that matches	Jain discloses the network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises configure the network provisioning instruction set so that when the traffic event possesses the characteristic that matches the first traffic classification filter and the characteristic that matches the second traffic classification filter, the first policy enforcement action has a higher priority than the second policy enforcement action. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 39. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

the second traffic classification filter, the first policy enforcement action has a higher priority than the second policy enforcement action.	
[40] The network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises configure the one or more traffic inspection provisioning instructions so that when the network traffic inspection system determines that the traffic event possesses the characteristic that matches the first traffic classification filter and the characteristic that matches the second traffic classification filter, the network policy enforcement system applies the first policy enforcement action but does not apply the second policy enforcement action.	Jain discloses the network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises configure the one or more traffic inspection provisioning instructions so that when the network traffic inspection system determines that the traffic event possesses the characteristic that matches the first traffic classification filter and the characteristic that matches the second traffic classification filter, the network policy enforcement system applies the first policy enforcement action but does not apply the second policy enforcement action. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 40. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[41] The network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic	Jain discloses the network service plan provisioning system of claim 1, wherein process the first service plan component and the second service plan component to create a network provisioning instruction set in accordance with a prioritization of the first traffic classification filter over the second traffic classification filter comprises configure the one or more traffic inspection provisioning instructions so that when the network traffic inspection system determines that the traffic event possesses the characteristic that matches the first traffic classification filter and the characteristic that matches the second traffic classification filter, the network policy enforcement system applies the

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

classification filter over the second traffic classification filter comprises configure the one or more traffic inspection provisioning instructions so that when the network traffic inspection system determines that the traffic event possesses the characteristic that matches the first traffic classification filter and the characteristic that matches the second traffic classification filter, the network policy enforcement system applies the first policy enforcement action before applying the second policy enforcement action.	first policy enforcement action before applying the second policy enforcement action. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 41. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[42] The network service plan provisioning system of claim 1, wherein the network policy enforcement system comprises a policy decision element.	Jain discloses the network service plan provisioning system of claim 1, wherein the network policy enforcement system comprises a policy decision element. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 42. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[43] The network service plan provisioning system of claim 1, wherein the network policy enforcement system or the network traffic inspection system comprises a gateway.	Jain discloses the network service plan provisioning system of claim 1, wherein the network policy enforcement system or the network traffic inspection system comprises a gateway. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 43. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

[44] The network service plan provisioning system of claim 1, wherein at least a portion of the network policy enforcement system is on the wireless end-user device	Jain discloses the network service plan provisioning system of claim 1, wherein at least a portion of the network policy enforcement system is on the wireless end-user device. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 44. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[45] The network service plan provisioning system of claim 1, wherein at least a portion of the network policy enforcement system is in a network system communicatively coupled to the wireless end-user device over the wireless access network.	Jain discloses the network service plan provisioning system of claim 1, wherein at least a portion of the network policy enforcement system is in a network system communicatively coupled to the wireless end-user device over the wireless access network. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 45. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[46] The network service plan provisioning system of claim 1, wherein the network traffic inspection system or the network policy enforcement system comprises a programmable element.	Jain discloses the network service plan provisioning system of claim 1, wherein the network traffic inspection system or the network policy enforcement system comprises a programmable element. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 46. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

[47] The network service plan provisioning system of claim 1, wherein the network policy enforcement system or the network traffic inspection system comprises a modem or an agent on the wireless end-user device.	Jain discloses the network service plan provisioning system of claim 1, wherein the network policy enforcement system or the network traffic inspection system comprises a modem or an agent on the wireless end-user device. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 47. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[57] The network service plan provisioning system of claim 1, wherein the network policy enforcement system comprises a notification element.	Jain discloses the network service plan provisioning system of claim 1, wherein the network policy enforcement system comprises a notification element. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 57. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[58] The network service plan provisioning system of claim 1, wherein the network policy enforcement system implements a notification function.	Jain discloses the network service plan provisioning system of claim 1, wherein the network policy enforcement system implements a notification function. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 58. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

[59p] The network service plan provisioning system of claim 58, wherein the one or more network elements are further configured to:	Jain discloses the network service plan provisioning system of claim 58, wherein the one or more network elements are further configured to. *See supra* claims 1, 58. In addition, Jain anticipates and/or renders obvious claim 59. *See supra* claims 1, 58. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[59a] obtain notification information, the notification information at least assisting to specify or identify a notification content, a notification trigger, or a notification offer; and	Jain discloses obtaining notification information, the notification information at least assisting to specify or identify a notification content, a notification trigger, or a notification offer. *See supra* claims 1, 58. In addition, Jain anticipates and/or renders obvious claim 59. *See supra* claims 1, 58. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[59b] determine at least a portion of the policy enforcement provisioning instructions based on the notification information.	Jain discloses determining at least a portion of the policy enforcement provisioning instructions based on the notification information. *See supra* claims 1, 58. In addition, Jain anticipates and/or renders obvious claim 59. *See supra* claims 1, 58. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[60] The network service plan provisioning system of claim 1, wherein the one or more policies comprise a notification policy.	Jain discloses the network service plan provisioning system of claim 1, wherein the one or more policies comprise a notification policy. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 60. *See supra* claim 1.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[61] The network service plan provisioning system of claim 60, wherein the one or more policy enforcement provisioning instructions assist in causing a notification to be delivered to a subscriber or to the wireless end-user device.	Jain discloses the network service plan provisioning system of claim 60, wherein the one or more policy enforcement provisioning instructions assist in causing a notification to be delivered to a subscriber or to the wireless end-user device. *See supra* claims 1, 60. In addition, Jain anticipates and/or renders obvious claim 61. *See supra* claims 1, 60. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[62] The network service plan provisioning system of claim 61, wherein the notification comprises a selection option for providing feedback or instructions.	Jain discloses the network service plan provisioning system of claim 61, wherein the notification comprises a selection option for providing feedback or instructions. *See supra* claims 1, 60, 61. In addition, Jain anticipates and/or renders obvious claim 62. *See supra* claims 1, 60, 61. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[63] The network service plan provisioning system of claim 61, wherein the notification indicates that a usage of a service plan has reached a particular percentage of a limit, or that a requested network activity has been	Jain discloses the network service plan provisioning system of claim 61, wherein the notification indicates that a usage of a service plan has reached a particular percentage of a limit, or that a requested network activity has been capped because a policy limit has been reached. *See supra* claims 1, 60, 61. In addition, Jain anticipates and/or renders obvious claim 63. *See supra* claims 1, 60, 61.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

capped because a policy limit has been reached.	To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[64] The network service plan provisioning system of claim 61, wherein the notification provides information about a service plan limit or an overage.	Jain discloses the network service plan provisioning system of claim 61, wherein the notification provides information about a service plan limit or an overage. *See supra* claims 1, 60, 61. In addition, Jain anticipates and/or renders obvious claim 64. *See supra* claims 1, 60, 61. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[65] The network service plan provisioning system of claim 61, wherein the notification provides information about an offer.	Jain discloses the network service plan provisioning system of claim 61, wherein the notification provides information about an offer. *See supra* claims 1, 60, 61. In addition, Jain anticipates and/or renders obvious claim 65. *See supra* claims 1, 60, 61. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[66] The network service plan provisioning system of claim 65, wherein the offer is an offer to allow an overage, an offer for a new service plan, or an offer to block an ongoing usage.	Jain discloses the network service plan provisioning system of claim 65, wherein the offer is an offer to allow an overage, an offer for a new service plan, or an offer to block an ongoing usage. *See supra* claims 1, 60, 61, 65. In addition, Jain anticipates and/or renders obvious claim 66. *See supra* claims 1, 60, 61, 65.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[68] The network service plan provisioning system of claim 61, wherein the notification provides information about an activity of the wireless end-user device that has been blocked, or an activity of the wireless end-user device that is not allowed.	Jain discloses the network service plan provisioning system of claim 61, wherein the notification provides information about an activity of the wireless end-user device that has been blocked, or an activity of the wireless end-user device that is not allowed. *See supra* claims 1, 60, 61.

In addition, Jain anticipates and/or renders obvious claim 68. *See supra* claims 1, 60, 61.

To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached. |
| | |
| [69] The network service plan provisioning system of claim 61, wherein the notification provides a message or an offer based on a current activity or a status of the wireless end-user device. | Jain discloses the network service plan provisioning system of claim 61, wherein the notification provides a message or an offer based on a current activity or a status of the wireless end-user device. *See supra* claims 1, 60, 61.

In addition, Jain anticipates and/or renders obvious claim 69. *See supra* claims 1, 60, 61.

To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached. |
| | |
| [70] The network service plan provisioning system of claim 69, wherein the current activity or the status of the wireless end-user device is based on the traffic event. | Jain discloses the network service plan provisioning system of claim 69, wherein the current activity or the status of the wireless end-user device is based on the traffic event. *See supra* claims 1, 60, 61, 69.

In addition, Jain anticipates and/or renders obvious claim 70. *See supra* claims 1, 60, 61, 69. |

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[71] The network service plan provisioning system of claim 61, wherein the notification is an actionable notification enabling a user of the wireless end-user device to provide a response to the notification.	Jain discloses the network service plan provisioning system of claim 61, wherein the notification is an actionable notification enabling a user of the wireless end-user device to provide a response to the notification. *See supra* claims 1, 60, 61. In addition, Jain anticipates and/or renders obvious claim 71. *See supra* claims 1, 60, 61. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[72] The network service plan provisioning system of claim 71, wherein the response comprises a directive to dismiss the notification, a directive to cancel the notification, an acknowledgment of the notification, a request for information, or a request to make a purchase.	Jain discloses the network service plan provisioning system of claim 71, wherein the response comprises a directive to dismiss the notification, a directive to cancel the notification, an acknowledgment of the notification, a request for information, or a request to make a purchase. *See supra* claims 1, 60, 61, 71. In addition, Jain anticipates and/or renders obvious claim 72. *See supra* claims 1, 60, 61, 71. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[80] The network service plan provisioning system of claim 61, wherein the notification comprises an upsell offer.	Jain discloses the network service plan provisioning system of claim 61, wherein the notification comprises an upsell offer. *See supra* claims 1, 60, 61. In addition, Jain anticipates and/or renders obvious claim 80. *See supra* claims 1, 60, 61.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[85] The network service plan provisioning system of claim 61, wherein the notification comprises information about a purchase, a data usage, an application, an amount of data, a percentage, or a combination of these.	Jain discloses the network service plan provisioning system of claim 61, wherein the notification comprises information about a purchase, a data usage, an application, an amount of data, a percentage, or a combination of these. *See supra* claims 1, 60, 61. In addition, Jain anticipates and/or renders obvious claim 85. *See supra* claims 1, 60, 61. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[86] The network service plan provisioning system of claim 61, wherein the notification comprises information to assist a subscriber in activating the wireless end-user device, selecting a service plan for the wireless end-user device, setting a preference, or a combination of these.	Jain discloses the network service plan provisioning system of claim 61, wherein the notification comprises information to assist a subscriber in activating the wireless end-user device, selecting a service plan for the wireless end-user device, setting a preference, or a combination of these. *See supra* claims 1, 60, 61. In addition, Jain anticipates and/or renders obvious claim 86. *See supra* claims 1, 60, 61. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[87] The network service plan provisioning system of claim 1, wherein the one or more policies comprise a traffic control policy.	Jain discloses the network service plan provisioning system of claim 1, wherein the one or more policies comprise a traffic control policy. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 87. *See supra* claim 1.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[88] The network service plan provisioning system of claim 87, wherein the control policy specifies to allow, block, throttle, delay, or defer the traffic event.	Jain discloses the network service plan provisioning system of claim 87, wherein the control policy specifies to allow, block, throttle, delay, or defer the traffic event. *See supra* claims 1, 87. In addition, Jain anticipates and/or renders obvious claim 88. *See supra* claims 1, 87. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[89] The network service plan provisioning system of claim 87, wherein the traffic control policy is based on a network state, a device state, a service-plan-usage state, or a combination of these.	Jain discloses the network service plan provisioning system of claim 87, wherein the traffic control policy is based on a network state, a device state, a service-plan-usage state, or a combination of these. *See supra* claims 1, 87. In addition, Jain anticipates and/or renders obvious claim 89. *See supra* claims 1, 87. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[90] The network service plan provisioning system of claim 1, wherein the traffic event is associated with a particular destination, a particular application on the wireless end-user device, a content type, a protocol, a	Jain discloses the network service plan provisioning system of claim 1, wherein the traffic event is associated with a particular destination, a particular application on the wireless end-user device, a content type, a protocol, a port, or an operating system of the wireless end-user device. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 90. *See supra* claim 1.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

port, or an operating system of the wireless end-user device.	To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[91] The network service plan provisioning system of claim 1, wherein the traffic event is associated with a specified remote destination, a specified application, a specified operating system, a specified content, a specified protocol, or a specified port number.	Jain discloses the network service plan provisioning system of claim 1, wherein the traffic event is associated with a specified remote destination, a specified application, a specified operating system, a specified content, a specified protocol, or a specified port number. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 91. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[92] The network service plan provisioning system of claim 91, wherein the specified remote destination is identified by a domain or an Internet protocol (IP) address.	Jain discloses The network service plan provisioning system of claim 91, wherein the specified remote destination is identified by a domain or an Internet protocol (IP) address. *See supra* claims 1, 91. In addition, Jain anticipates and/or renders obvious claim 92. *See supra* claims 1, 91. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[93] The network service plan provisioning system of claim 91, wherein the specified application is identified by a name, a hash, a certificate, or a signature.	Jain discloses the network service plan provisioning system of claim 91, wherein the specified application is identified by a name, a hash, a certificate, or a signature. *See supra* claims 1, 91. In addition, Jain anticipates and/or renders obvious claim 93. *See supra* claims 1, 91.

57

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

	To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[96] The network service plan provisioning system of claim 1, wherein the first service plan component or the second service plan component comprises a carrier component, a network protection component, an application component, a sponsored component, a subscriber-paid component, a marketing interceptor component, a parental control component, a bulk component, a post-bulk component, or an end-of-life component.	Jain discloses the network service plan provisioning system of claim 1, wherein the first service plan component or the second service plan component comprises a carrier component, a network protection component, an application component, a sponsored component, a subscriber-paid component, a marketing interceptor component, a parental control component, a bulk component, a post-bulk component, or an end-of-life component. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 96. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[98] The network service plan provisioning system of claim 1, wherein the first service plan component or the second service plan component is associated with a service class.	Jain discloses the network service plan provisioning system of claim 1, wherein the first service plan component or the second service plan component is associated with a service class. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 98. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[99] The network service plan provisioning system of claim 98, wherein the service class is paid, marketing intercept, carrier, network	Jain discloses the network service plan provisioning system of claim 98, wherein the service class is paid, marketing intercept, carrier, network protection, sponsored, parental control, open access, bulk, post-bulk, or a combination of these. *See supra* claims 1, 98.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

protection, sponsored, parental control, open access, bulk, post-bulk, or a combination of these.	In addition, Jain anticipates and/or renders obvious claim 99. *See supra* claims 1, 98. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[112] The network service plan provisioning system of claim 1, wherein the information specifying the first traffic classification filter or the information specifying the second traffic classification filter comprises a name, a description, a filtering parameter, a launch mechanism, or a combination of these.	Jain discloses the network service plan provisioning system of claim 1, wherein the information specifying the first traffic classification filter or the information specifying the second traffic classification filter comprises a name, a description, a filtering parameter, a launch mechanism, or a combination of these. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 112. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[113] The network service plan provisioning system of claim 112, wherein the filter parameter specifies filtering the traffic event by destination, by application, by operating system, by protocol, or by port.	Jain discloses the network service plan provisioning system of claim 112, wherein the filter parameter specifies filtering the traffic event by destination, by application, by operating system, by protocol, or by port. *See supra* claims 1, 112. In addition, Jain anticipates and/or renders obvious claim 113. *See supra* claims 1, 112. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[120] The network service plan provisioning system of claim 1, wherein the one or more policies comprise a	Jain discloses the network service plan provisioning system of claim 1, wherein the one or more policies comprise a policy associated with a tethering function. *See supra* claim 1.

Exhibit B-1 – Invalidity of U.S. Patent No. 8,924,543 in view of Jain

policy associated with a tethering function.	In addition, Jain anticipates and/or renders obvious claim 120. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.
[121] The network service plan provisioning system of claim 1, wherein the one or more policies comprise a policy associated with a web page, a domain, an application, a roaming network, an e-mail service, a networking service, a music download service, a video game service, a multimedia service, or a combination of these.	Jain discloses the network service plan provisioning system of claim 1, wherein the one or more policies comprise a policy associated with a web page, a domain, an application, a roaming network, an e-mail service, a networking service, a music download service, a video game service, a multimedia service, or a combination of these. *See supra* claim 1. In addition, Jain anticipates and/or renders obvious claim 121. *See supra* claim 1. To the extent Jain does not explicitly and/or inherently disclose this element, it would have been obvious in view of the knowledge of a person of ordinary skill in the art in light of Jain alone or it would have been obvious to combine Jain with one or more prior art references charted in these Invalidity Contentions or identified in the cover document to which this chart is attached.